The Honorable Robert S. Lasnik

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

| | |
|---|---|
| UNITED STATES OF AMERICA,<br>Plaintiff,<br>v.<br>PAIGE A. THOMPSON<br>Defendant. | NO. CR19-159 RSL<br>**GOVERNMENT'S TRIAL BRIEF** |

## I. INTRODUCTION

Paige Thompson is charged in a 10-count Second Superseding Indictment with wire fraud, numerous violations of the Computer Fraud and Abuse Act, access device fraud, and aggravated identity theft. The charges stem from Thompson's scheme to hack cloud computing customers who had misconfigured their web application firewalls. Once Thompson identified cloud customers whose internal resources were vulnerable, she stole the security credentials associated with those resources. She then used the stolen security credentials to: (1) steal data from the cloud customers and (2) steal computing power to mine cryptocurrency (a cybercrime commonly referred to as "cryptojacking").

Thompson's trial is scheduled to start on June 7, 2022, at 9:00 a.m. The United States will be represented by Assistant United States Attorneys Andrew C. Friedman,



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Jessica M. Manca, and Tania M. Culbertson. The case agent at trial will be Federal Bureau of Investigation Special Agent Joel Martini. Thompson is represented by Mohammad Hamoudi, Christopher Sanders, Nancy Tenney, Brian Klein, Melissa Meister, and Emily Stierwalt.

Thompson has been released on bond, pending trial. A defense motion to reconsider the Court's Order Denying Motion to Dismiss Counts 2 Through 8 (Mar. 21, 2022, Dkt. 226) is pending; the Court has not requested a response from the United States. *See* Dkt. 240. A defense motion to exclude evidence pursuant to Rule 404(b) is also pending and noted for Friday, May 27, 2022. *See* Dkt. 242.

The United States expects to call approximately 20 witnesses during its case-in-chief. The United States anticipates that it will be able to present its case-in-chief in six or seven days, assuming reasonable cross-examination by the defense.

## II. BACKGROUND

### A. Facts

*The Basics of Cloud Computing Architecture*

In earlier stages of the computer age, customers purchased, stored, and maintained their own computer hardware within their own office spaces. Within the past 20 years, as technology has developed and industries rely more heavily on computing resources, many companies have transitioned to a "pay-as-you-go" model of computer hardware and software, sometimes referred to as "hardware-as-a-service" and "software-as-a-service." For a usage-based fee, companies like Amazon Web Services (AWS) provide access to computing resources that AWS physically maintains in its numerous data centers across the world. Through this model, computing resources are housed in shared data centers that support thousands, if not millions, of customers, rather than in each company's individual local data center. By tapping into remote computing resources, companies can quickly increase or decrease their usage as needed (a concept referred to



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

as "scalability"). Providing off-site computing resources as a pay-as-you-go service is commonly referred to as "cloud computing."

AWS manages the security of its cloud infrastructure for its customers through its Identity and Access Management (IAM) products. IAM is a fundamentally important security function within AWS that provides authentication and authorization mechanisms for AWS services. Every action on AWS requires a user to authenticate into an AWS account through the IAM system. When authentication is based on identity, security is premised on the concept of the user being who they claim to be.

By default, all access is denied under the IAM system, and a customer must create policies and permissions that grant access. There are different kinds of identities that can be used to access resources on AWS. Identities are meant to be assumed and used only by entities that are authorized to assume and use them. One type of identity is an IAM user, which is an identity with long-term security credentials, such as a username and password. Another type of identity is an IAM role, which is an identity with a set of short-term security credentials that the role uses to perform functions on AWS resources. The IAM role's security credentials include an access key, a secret access key, and a token. There are other kinds of security mechanisms that can provide access to AWS services as well, such as security groups and keypairs.

By default, IAM roles have no permissions. AWS customers assign permissions to IAM roles that allow the roles to perform certain functions within the AWS environment. Before an IAM user, application, or service can use an IAM role and its associated security credentials, an authorized IAM user must grant that entity permission to assume the role. The entities that use IAM roles are often machines or programs running on the AWS infrastructure, not people. When an application uses an IAM role to access an AWS service, this is referred to as a "service role." For example, a billing software program might need access to a specific database to generate invoices. A



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

company can assign an IAM role to its billing program that will allow the program to access the necessary database.[1]

Another more technical aspect of AWS's cloud infrastructure is AWS's metadata service. Metadata is "information about information," such as the information associated with a digital photograph that shows when the photograph was taken, where it was taken, and what kind of device took the photograph. AWS's metadata service provides information about its virtual computers, such as "Which AWS account is this resource associated with?" and "Which IP address is connected to this resource?" and, most critically, "Which security credentials are used to access this resource?" This metadata information is stored on software, hardware, or firmware called a "hypervisor," which manages the thousands of virtual computers running on AWS's hardware. When a virtual machine needs information about itself, it sends an internal request to the hypervisor. There is a hypervisor installed on every piece of hardware in AWS's data centers. Information in the hypervisor is private, and information about the hypervisor is only available to someone operating within the AWS client's internal environment, meaning on or in a virtual machine.

*The Basics of Internet Architecture*

When a person ("client") surfs the Internet, he or she commonly uses a web browser like Internet Explorer, Google Chrome, or Mozilla Firefox, to contact a web server to retrieve information. When the request reaches the web server, the server may accept the request and look for the requested information on its hosted website. If the information is located locally on the web server, the web server sends the information back to the web browser. Sometimes the information may need to be obtained from back-end or internal servers, not accessible by external hosts on the Internet. The web

[1] In the AWS world, stored files and folders are referred to as "objects," and objects are stored in database containers called "S3 buckets." "Amazon S3" is an abbreviation for "Amazon Simple Storage Service," which is a cloud storage service that AWS provides to its customers.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

server will route the request to look for the request on the back-end servers. Once the information is found, it is routed back to the web server and sent back to the web browser that requested the information, often without the web browser knowing that the information came from an internal, back-end server. This process of forwarding an external host's requests is referred to as a "reverse proxy."

A company can place a software application referred to as a "web application firewall" or "WAF" on its web server to add a layer of security protection. The WAF typically sits behind the network firewall on a private network, and it filters Internet traffic that attempts to access the web server. If the WAF is configured correctly, it can protect the web server and other internal resources by hiding their identities from external hosts and protecting them from common cyberattacks, such as server-side request forgeries.[2]

*The Vulnerability Thompson Exploited*

The companies that Thompson breached had a common issue: their web application firewalls (WAFs) were misconfigured in a way that allowed an external user to make reverse proxy requests. In other words, instead of simply filtering Internet traffic destined for the web server, the WAF was also able to issue its own proxy requests for information from internal resources. The internal resources recognized the WAF as a trusted internal source and provided the information that the WAF requested. This configuration left the WAF vulnerable to an external user like Thompson, who was able to exploit the trusted relationship between the WAF and the internal metadata service. Thompson used the WAF to request internal information that would not normally be available to, and was not intended to be available to, an external user. She was able to exploit this vulnerability in part because she accessed the WAF through a Linux

[2] A server-side request forgery is a common form of cyberattack in which a hacker tricks a web server into making requests on his or her behalf, thereby allowing the hacker to gain access to internal resources that he or she does not have permission to access.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

command-line tool for sending and receiving data using various network protocols, rather than through the normal Internet browser HTTP and HTTPS protocols that the WAF and the web server were expecting.

As set forth in greater detail below, Thompson used misconfigured WAFs to make reverse proxy requests for internal metadata of AWS customers. The internal metadata service mistakenly believed that the request was coming from a trusted identity (*i.e.* the WAF), and provided the metadata that the WAF requested on Thompson's behalf. This internal metadata included information about the security credentials used to access AWS resources. In this case, Thompson was seeking a specific security credential: the IAM role used by the web server and its associated applications to access the metadata service. Once she acquired information about the IAM role, she assumed the role and used its security credentials to perform other functions in AWS's cloud environment, such as listing and syncing (downloading) buckets and creating security groups, keypairs, and new instances that would help her install and run her cryptocurrency mining programs.

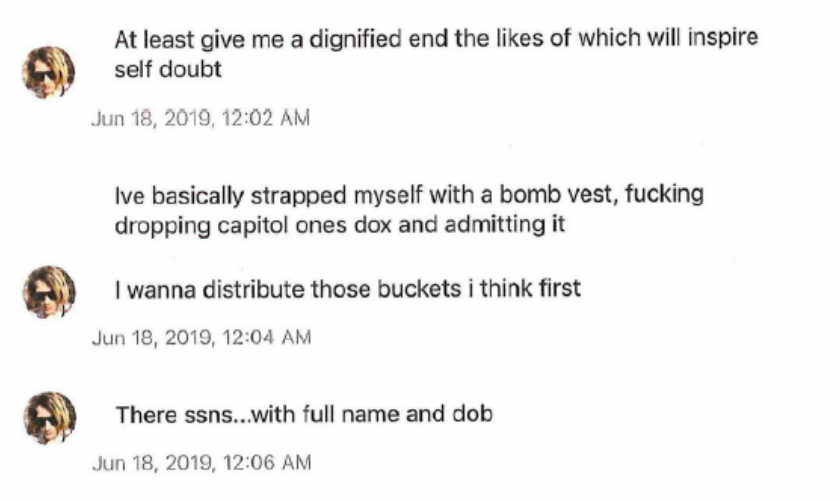
*A Responsible Disclosure to Capital One*

In June 2019, a woman, identified herein by her initials, K.V., received a series of unsolicited private Twitter messages from a Twitter account later found to belong to Thompson. Thompson was a complete stranger to K.V.; the two had never spoken to one another or even chatted online before. Thompson said she was "gonna dox" herself[3], provided a series of hyperlinks to posts on the website GitHub, claimed to have "3tb of s3 buckets" that she "jacked," and said that she was "gonna give it all to this desperate Chinese dude who scams people for research chems on reddit and drug forums." Thompson also wrote:

[3] "Doxxing" is publicly broadcasting private information in an online forum, often with malicious intent.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970




K.V. told Thompson that she was not a snitch and that Thompson could report herself to the FBI. Then, K.V. blocked Thompson on Twitter.

K.V. anguished over what to do with the information she had received from Thompson. In online culture, particularly hacker culture, there is a strong bias against reporting other hackers' activities to law enforcement, or "snitching." But K.V. was also deeply troubled by Thompson's possession of people's personal identifying information and Thompson's threat to distribute that all of that information to a scammer. On July 17, 2019, K.V. decided that she had to notify Capital One about the potential data breach.

Like many large companies, Capital One encourages security researchers to report potential security vulnerabilities, and their website has a detailed explanation of how to do so. Capital One does not operate a public "bug bounty program", that is, it does not pay security researchers for finding and disclosing potential vulnerabilities. K.V. looked up information about Capital One's responsible disclosure program. She saw an email address prominently listed on Capital One's responsible disclosure webpage ("responsibledisclosure@capitalone.com"), and sent the company an email.

K.V.'s email contained a hyperlink to one of Thompson's posts on GitHub, which is an online computer code hosting platform where people can work on computer coding projects, including by storing code, sharing code, and collaborating on coding with others. Coding posts on GitHub that can be shared with others are referred to as "gists."



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Gists can be public or private, depending on the user's preferences. If they are private, then the user needs the precise hyperlink to access the gist. The gists in this case were private; however, K.V. provided the private hyperlink given to her by Thompson. This hyperlink allowed Capital One to view Thompson's private gist.

The gist contained computer code and a long list of private S3 buckets (data repositories) that belonged to Capital One. The computer code included the command to assume and use Capital One's IAM role. When Capital One security professionals saw the gist via K.V.'s responsible disclosure email, they quickly realized the scope and seriousness of the data breach.

K.V. did not expect to be paid for her disclosure and did not accept any payment, even though Capital One offered to pay her. Instead, at K.V.'s request, Capital One made a sizable donation to two non-profit technology organizations, specifically, the Diana Initiative, which strives to improve diverse representation in the Information Security profession, and the Electronic Frontier Foundation (EFF), which advocates for digital privacy, free speech, and technological innovation.

*Identification of Paige Thompson*

Through open-source Internet research, Capital One quickly identified Paige Thompson as the likely creator of the GitHub gist and as the owner of the Twitter account that communicated with K.V. To begin, the username of the GitHub account was "paigeadelethompson." Among other pieces of identifying information, Thompson had posted a copy of her resume on a website linked to the GitHub page, and the resume listed her residential address in Seattle. Additional information confirmed that the accounts did in fact belong to Thompson. Capital One quickly referred its information about Thompson and the data breach to the FBI.

*FBI Search Warrant of Thompson's Residence*

Aware that Thompson had threatened to distribute Capital One's data, FBI worked quickly to obtain a federal search warrant for Thompson's residence. On July 29, 2019, less than two weeks after K.V. reported the breach to Capital One, the FBI served a



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

search warrant at Thompson's house and arrested her. During the search, the FBI seized a variety of devices from her bedroom, including an unusually large, custom-built desktop computer, a laptop, and an iPhone.

Before seizing Thompson's desktop computer, the FBI captured and preserved files that were available while the computer was active. In doing so, the FBI located a file directory titled "aws_dumps." This directory contained an archive of data stolen from companies throughout the world, including Capital One.

At her house, Thompson agreed to waive her constitutional rights and speak to the investigating FBI agents. Thompson told the FBI that she did not use iPredator's virtual private network (VPN) or the Onion Router (TOR)—which are both methods for anonymizing internet traffic—which was false. She did admit that she owned a GitHub account with the username paigeadelethompson, but claimed that she did not have any recent GitHub projects.

Thompson admitted that she found a misconfiguration that enabled her to access AWS services. She said that her activities exposed sensitive data, and she described the security vulnerability as "disturbing." Thompson falsely claimed that she did not remember whether she had downloaded or "synced" the sensitive data, that she did not try to look at the content of the data, and that she had probably deleted the data. She also falsely stated that she would not have put the data on her server. The FBI asked whether Thompson had contacted anyone about the vulnerability, and Thompson said she had contacted only one person, a former Amazon co-worker.

Later in the interview, Thompson admitted that she used iPredator and TOR to access the Capital One data. But she continued to falsely claim that nothing related to Capital One was on her GitHub account. Then, she revised her previous statement to admit that she downloaded Capital One's data onto her encrypted file server, and she provided agents with the encryption key. Thompson said that the downloaded Capital One data was located in a directory titled "aws_dumps." Thompson admitted that she



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

downloaded data from companies other than Capital One, but she said that the data was stored locally and never uploaded to an online storage service or sent to anyone else.

*Thompson's Hacking Scheme*

The evidence on Thompson's computer establishes that she took the following steps to hack victim companies. First, she anonymized her Internet identity using both a virtual private network (VPN) and The Onion Router (TOR). Second, she scanned millions of publicly available IP addresses hosted by AWS, looking for misconfigured web-facing applications that allowed her to communicate with a company's internal servers.

Third, when she found such misconfigured web applications, she tricked these applications into making internal requests on her behalf. This technique is a variation on a "server-side request forgery," and it is a common form of cyberattack. The request these web-facing applications made on Thompson's behalf was essentially asking if she could access an internal resource on AWS (the instance metadata service), and, if so, requesting internal user data about that resource—including security credentials used to access the resource. The internal user data obtained from the AWS metadata service included the name of the web application's IAM role.

Fourth, once Thompson acquired the name of an application's IAM role, she used the security credentials attached to that role to authenticate into a temporary session with the victim company's internal servers. Fifth, Thompson used the IAM role's permissions to perform actions in the victim company's cloud environment, such as viewing and copying data, or creating instances (servers), security groups, keypairs, and secured pathways to plant and run cryptocurrency mining programs.

Significantly, Thompson's precise methodology evolved somewhat over time. The evidence on Thompson's computer shows that Thompson often required multiple efforts to accomplish each of the steps described above. Over time, Thompson corrected, improved, streamlined, and automated code to improve upon its functionality or perform additional actions against an AWS server with less manual involvement.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

There is evidence that Thompson attacked some of the same companies multiple times. Sometimes, she stole their data and then later used their accounts to mine cryptocurrency, generating large AWS bills on the companies' accounts in the process. Other times, she returned to cryptojack the same company she had attacked weeks before, and wrote herself a digital note that the company had failed to fix its vulnerability. When possible, Thompson used stolen IAM roles to create keypairs, so that she could have another pathway to access a company's AWS resources even after they fixed the vulnerability that allowed her access their resources in the first place.

*The Scope of the Breach*

Analysis of Thompson's computer showed that Thompson scanned tens of millions of AWS customers looking for vulnerabilities. She stole data not only from Capital One, but also from at least 30 other entities. After breaching Capital One, she exfiltrated the personal identifying information of over 100 million people—roughly one-third of the United States' adult population—constituting one of the largest data breaches in United States' history.

*Thompson's Motives*

Consistent with Thompson's statement on the day of her arrest, the FBI has no reason to believe that Thompson distributed the data that she downloaded or that she uploaded it to an external storage service. But there is ample evidence that she was actively looking for an opportunity to do so.

Shortly after downloading the Capital One data in March 2019, Thompson searched the data for personal identifying information of people who had addresses in Seattle. She created a list of Seattle residents' personal identifying information that she named the "Capitol_One_Inclusion_List." Then, she took the personal identifying information of one of the people on that list, J.B., and put it into a file she named "id." J.B.'s personal identifying information also appears in an autofill field on Thompson's phone.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

For several months, Thompson thought about what she would do with the terabytes of data she had downloaded. By May 2019, Thompson was searching for credit card algorithms and terms like "carding forums dark web." On June 5, 2019, she told a friend that she was "thinking about carding alot [sic] lately." Around the same time, Thompson's Internet history shows that she looked into renting servers in Russia. A few weeks later, she messaged K.V., threatening to distribute terabytes of data to a scammer.

In late June, she was still looking for a place to store the stolen data:


A few days later, Thompson threatened to upload the data to "mega" (a cloud-based storage service) and "give it to an avid scammer, a chinaman who will find a good perm home for it on the black markt [sic], sealed with the story behind it." On July 14, only a few days before K.V.'s responsible disclosure to Capital One and two weeks before her



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

arrest, Thompson wrote to a friend:

2019-07-14.log

```
663  [07:54:12] <erratic> lol
664  [07:56:30] <erratic> kongfuzi: you got a place I can upload 2.2TB of stuff
665  [07:56:52] <erratic> I cant really talk about what it is or how I got it
666  [07:56:58] <erratic> its just stuff
667  [07:57:05] <erratic> you know how it goes
```

One of the reasons Thompson did not help companies fix their vulnerability was that her hacking scheme was profitable to her. She frequently boasted of a "cryptojacking enterprise" that made her several thousand dollars a month. She knew that downloading other companies' information and using their computing power was illegal, but she did not care. She told a friend:


In mid-July, Thompson explained her hacking scripts to a friend and then wrote:

```
[11:51:32] <erratic> but yeah if you just wanna use it to learn how to do some
shit with aws go for it its not my shit lol
```

Thompson's complete lack of interest in helping the companies she attacked is a significant part of the reason that she is not a "white hat hacker." Even if her actions could be broadly characterized as "research," she did not act in good faith. Rather, the evidence shows that she knew what she was doing was wrong, and she knew that she was exploiting a vulnerability that companies did not know they had. She was motivated both to make money and to gain notoriety in the hacking community and beyond. What she was not motivated by was an interest in making cloud computing safer or more secure.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

**B. Procedure**

Thompson was charged by complaint on the day of her arrest, July 29, 2019. Dkt. 1. She was detained at the Federal Detention Center for approximately 14 weeks. *See* Dkt. 32. On November 4, 2019, the Court granted a defense motion to review Thompson's detention order and released her on a pretrial appearance bond. *See* Dkt. 67.

On August 28, 2019, Thompson was indicted. Dkt. 33. The grand jury returned a Superseding Indictment on June 17, 2021, and a Second Superseding Indictment on January 12, 2022. Dkt. 102, 166.

The Second Superseding Indictment charges Thompson with the following offenses:

- Count 1 – Wire Fraud, in violation of 18 U.S.C. § 1373.
- Counts 2 to 5 – Computer Fraud and Abuse (Unauthorized Access > $5,000), in violation of 18 U.S.C. § 1030(a)(2)(C), and (c)(2)(A) and (B)(iii).
- Counts 6 and 7 – Computer Fraud and Abuse (Unauthorized Access < $5,000), in violation of 18 U.S.C. § 1030(a)(2)(C) and (c)(2)(A).
- Count 8 – Computer Fraud and Abuse (Damage to a Protected Computer), in violation of 18 U.S.C. § 1030(a)(5)(A) and (c)(4)(B)(i).
- Count 9 – Access Device Fraud, in violation of 18 U.S.C. § 1029(a)(3), (b)(1), and (c)(1)(a)(i).
- Count 10– Aggravated Identity Theft, in violation of 18 U.S.C. § 1028A(a)(1).

## III. ELEMENTS OF THE OFFENSES

**A. Wire Fraud**

Count 1 charges Thompson with Wire Fraud. The elements of Wire Fraud are:

*First*, beginning in or before March 2019 and continuing until on or about July 17, 2019, the defendant knowingly participated in, devised, or intended to devise a scheme or



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

plan to defraud, or a scheme or plan for obtaining money or property by means of false or fraudulent pretenses, representations, or promises;

*Second*, the statements made or facts omitted as part of the scheme were material; that is, they had a natural tendency to influence, or were capable of influencing, a person to part with money or property;

*Third*, the defendant acted with the intent to defraud, that is, the intent to deceive and cheat; and

*Fourth*, on or about March 22, 2019, the defendant used, or caused to be used, an interstate or foreign wire communication to carry out or attempt to carry out an essential part of the scheme.

The government will prove this charge at trial by showing that Thompson took advantage of AWS clients who had misconfigured their web application firewalls to steal security credentials for the clients' IAM roles. The government will prove that Thompson then issued commands—that she implicitly represented were commands issued by legitimate users with permission to send such commands (rather than commands sent by a person who had stolen the credentials—to defraud the victims of two things: (1) data stored by the victims, and (2) computing power that Thompson used to mine cryptocurrency for her own benefit.

**B. Computer Fraud and Abuse – Obtaining Information**

Counts 2 and 4-7 each charge Thompson with accessing computers without authorization and obtaining information from that computer. The elements of these counts vary, depending upon the type of victim and the value of the information Thompson took. The elements of Count 2 (which relates to Capital One) are:

*First*, between on or about March 12, 2019, and on or about July 17, 2019, the defendant intentionally accessed without authorization a computer;

*Second*, by accessing without authorization a computer, the defendant obtained information contained in a financial record of a financial institution or of a card issuer; and



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

*Third*, the value of the information obtained exceeded $5,000.

The elements of Counts 4 and 5 (which related to Apperian and Survox), are:

*First,* on or about the dates charged in the Indictment, the defendant intentionally accessed without authorization a computer;

*Second*, by accessing without authorization a computer,the defendant obtained information from a computer that was used in or affecting interstate or foreign commerce or communication; and

*Third*, the value of the information obtained exceeded $5,000.

The elements of Counts 6 and 7 (which relate to Bitglass and 42 Lines, Inc.) are the same as those for Counts 4 and 5, except that the government is not required to show the third element, namely that the value of the information exceeded $5,000.

The government will prove these charges at trial by showing that Thompson obtained information from each of the companies that is the subject of these charges. FBI Computer Scientist Waymon Ho will testify concerning computer scripts found on Thompson's computer that Thompson used to gain access, without authorization, to each of the victims' computers. Mr. Ho also will testify that data belonging to each of the victims was found on Thompson's computer. Witnesses from each of the companies will confirm that the data belongs to their companies, and that Thompson was not authorized to access the companies' computers. The government also will introduce evidence that Thompson bragged repeatedly on social media and in communications with others that she had stolen the data.

The victim charged in Count 3 is a company headquartered outside the United States that no longer wishes to assist with the prosecution. Therefore, the government will move to dismiss Count 3 before trial. Pursuant to the government's prior notices, the government intends to present evidence that this company was one of the victims of Thompson's hacking scheme.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

**C. Computer Fraud and Abuse – Damaging Computers**

Count 8 charges Thompson with accessing computers without authorization and with impairing or damaging those computers. The elements of this crime are:

*First*, beginning on or about March 10, 2019, and continuing until on or after August 5, 2019, the defendant knowingly caused the transmission of a program, information, code, or command to a computer;

*Second*, as a result of the transmission, the defendant intentionally impaired without authorization the integrity or availability of data, a program, a system, or information;

*Third*, the computer was used in or affected interstate or foreign commerce or communication; and

*Fourth*, the offense caused loss to one or more persons, during a one-year period, including loss from a related course of conduct, aggregating at least $5,000 in value.

The government will prove this charge at trial by showing that Thompson planted cryptocurrency-mining software on computers belonging to a number of companies, including named victim Survox. The evidence that Thompson planted this software includes evidence that: (1) Thompson's computer contained scripts designed to plant cryptocurrency-mining software on computers of AWS customers with identifiable IP addresses; (2) some of those customers, including Survox, had new instances (servers) opened on their accounts that they had not ordered; (3) more than $10,000 of Ether (a type of cryptocurrency) was deposited into the wallet identified in Thompson's mining scripts between March 10, 2019, and August 5, 2019, and (4) Thompson bragged repeatedly on social media and in texts and direct messages that she was engaged in cryptojacking.

**D. Access Device Fraud**

Count 9 charges Thompson with access device fraud. The elements of this crime are:



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

*First*, beginning on or about March 12, 2019, and continuing until on or about July 17, 2019, the defendant knowingly possessed or attempted to possess at least fifteen unauthorized access devices at the same time;

*Second*, the defendant knew that the devices were unauthorized;

*Third*, the defendant acted with the intent to defraud, that is, the intent to deceive and cheat; and

*Fourth*, the defendant's conduct in some way affected commerce between one state and another state or states, or between a state of the United States and a foreign country.

The government will prove this crime at trial by showing that, after Thompson stole more than 100,000,000 million individuals' personally identifiable information (PII), Thompson took numerous steps that showed an intent to use the information herself, or to disseminate it to others, for use in committing credit card fraud, or other similar fraud. Thompson's computer search history shows that, after stealing the PII, she searched for numerous items related to committing credit card fraud, including information about the algorithms used to create credit card numbers, credit card embossers, and carding forums on which individuals can sell and purchase PII for use in credit card fraud. Thompson also manipulated PII data—for instance by creating a spreadsheet grouping information of Seattle residents—in a manner consistent with intending to use the information for fraudulent purposes. And, Thompson repeatedly threatened to upload the data to remote servers and give the information to scammers. But for the FBI's quick action to arrest Thompson and recover the data, it is likely that she would have used the information to commit credit card, or other fraud, using the information.

**E. Aggravated Identity Theft**

Count 10 charges Thompson with aggravated identity theft. The elements of this crime are:



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

*First*, the defendant knowingly transferred, possessed, or used without legal authority a means of identification of another person; and

*Second*, the defendant knew that the means of identification belonged to a real person; and

*Third*, the defendant did so during and in relation to the Access Device Fraud alleged in the indictment.

The government will prove this by showing that Thompson possessed more than 100,000,000 people's means of identification, and that she possessed that information during and in relation to the Access Device Fraud with which Thompson is charged in Count 9.

## IV. OTHER ISSUES

### A. Digital Evidence

The government intends to offer into evidence materials seized during the search of Thompson's computer. Because the entire computer contains nearly 20 terabytes of information, and because a complete image of the computer would not be useful to the jury, the government will offer file directories that list the filepaths for particular relevant evidence. The government also will offer folders and files that contain relevant evidence, including computer scripts that Thompson used to commit her crimes, folders or files containing information assembled as part of those crimes (such as information relating to roles associated with victims, and stolen by Thompson), and folders or files containing data stolen from victims. In some cases, the government will offer screenshots that capture part of the information in a folder or file (such as actual computer scripts or portions of stolen data). FBI Computer Scientist Waymon Ho will authenticate all of these materials as being materials that he found on Thompson's computer during his forensic examination of the computer.

### B. Evidence Offered Pursuant to Federal Rule of Evidence 902(11), (13) & (14)

The government also will offer into evidence materials obtained from Twitter, Google, Slack, and Github for accounts belonging to Thompson. These include the social



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

media postings and the communications described in Part II, above. The records are business records, records generated by an electronic process and/or records copied from electronic storage media. The government obtained, and has provided to the defense, the appropriate certifications pursuant to Federal Rule of Evidence 902 to establish that these documents are self-authenticating. The government anticipates that the defense will agree that they are authentic. To the extent that the defense does not agree, the government has addressed the issue in its Filing in Advance of Status Conference, Docket No. 251, and will request a hearing prior to trial to obtain rulings on the authenticity of these documents.

**C. Expert Testimony**

Although the defense declined to request expert discovery from the government, in order to avoid providing its own expert discovery, the parties have agreed to include in their trial briefs short summaries of the expert witnesses they intend to call, and the testimony they expect those witnesses to provide. The government expects to present testimony from five expert witnesses:

- Waymon Ho is an FBI Forensic Computer Scientist. Mr. Ho will testify concerning his forensic examination of Thompson's principal computer and other digital devices. Among other things, Mr. Ho will testify concerning computer scripts that he identified on that computer to execute each of the steps of Thompson's scheme to hack into servers belonging to AWS clients in order to steal data from those servers and to install cryptocurrency-mining software on the servers. Mr. Ho also will testify concerning data that he found on Thompson's computer that had been stolen from victims.

- John Strand is the founder of Black Hills Information Security, a technology firm that specializes in penetration testing. Mr. Strand is a nationally recognized expert on ethical hacking who will testify about industry terms, common practices, and ethical norms within the computer security community. Among other topics, Mr. Strand will define the terms "white hat hacker," "grey hat hacker,"



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

and "black hat hacker." He will testify that the accepted norms of the ethical hacking community include obtaining permission and stopping short of exploiting vulnerabilities. Accepted norms of the ethical hacking community also prohibit security researchers from copying others' data and from storing that information. Mr. Strand also will testify that accepted norms of the ethical hacking community prohibit engaging in conduct such as cryptojacking.

Mr. Strand will testify that Thompson's conduct violated these norms, and that her use of victim role credentials would be considered "black hat hacking." Mr. Strand also will testify about the different standards, within different parts of the security community, as to what type of disclosure of vulnerabilities is appropriate. Mr. Strand will testify that Thompson's bragging to a few individuals about her conduct failed to meet any of these varying standards for responsible disclosure.

- Kenneth Henderson is a Special Agent with the Secret Service. Mr. Henderson will testify concerning credit card fraud, including how persons commit credit card fraud and carding forums where people exchange and sell items necessary for credit card fraud (including stolen personally identifiable information). Among other things, Mr. Henderson will explain terms in web searches conducted by Thompson, such as "carding forums dark web." Mr. Henderson will testify how the information stolen by Thompson from Capital One could have been used to commit credit card fraud. And, Mr. Thompson also will testify that the information had a value, for criminal purposes, that far exceeded $5,000.

- Vincent Kenney is an FBI Computer Scientist. Mr. Kenney will testify concerning cryptocurrency and in particular, Ether. Among other things, Mr. Kenney will testify about the process of cryptocurrency mining, and about mining pools, and in particular Nanopool. Mr. Kenney also will testify about the phenomenon of



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

cryptojacking. Mr. Kenney also will testify about the amounts of cryptocurrency deposited into Thompson's Ether wallet, and the dates and date range on which deposits were made, and source of the deposits.

- Kenneth Muscatel is a forensic psychologist. In the event that Thompson offers expert testimony pursuant to Federal Rule of Criminal Procedure 12.2, Dr. Muscatel will offer testimony (presumably in rebuttal). Dr. Muscatel will testify concerning the examination of Thompson that he performed pursuant to the Court's order. Dr. Muscatel currently is preparing a report of that examination. Dr. Muscatel's examination and report have been delayed by the fact that Thompson did not provide notice of a mental health defense until after the motions deadline, and that, even then, Thompson chose not to submit to a mental health examination until ordered by the Court.

  The government will provide Dr. Muscatel's report to the defense when it receives the report. The government anticipates that the report will conclude, and Dr. Muscatel will testify, that Thompson does not suffer from any psychotic disorder, but that she does suffer from a mood disorder and a personality disorder. The government further anticipates that the report will conclude that these conditions did not prevent Thompson from being able to engage in a sustained effort over a substantial time to conduct a sophisticated hacking scheme, or from understanding what she was doing.

**D. Statements of the Defendant**

The government intends to introduce evidence regarding numerous statements made by Thompson on social media, or in text or direct messages to others. A defendant's own statements are admissible, non-hearsay admissions of a party-opponent when offered into evidence by the United States. *See* Fed. R. Evid. 801(d)(2)(A).

The government may offer all, some, or none of a defendant's statements at trial under Rule 801(d)(2). A defendant, however, cannot use this rule to offer her *own* prior



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

out-of-court statements. Rule 801(d)(2) is unavailable to a defendant, since she would be the proponent of the evidence and, where she seeks to introduce it, it is not offered against her. *United States v. Ortega*, 203 F.3d 675, 682 (9th Cir. 2000); *United States v. Fernandez*, 839 F.2d 639, 640 (9th Cir. 1988). As a result, the hearsay rule bars a defendant from introducing her own prior statements. *United States v. Mitchell*, 502 F.3d 931, 964-65 (9th Cir. 2007).

If the defendant wishes to tell her "side" of the story, she must take the stand and testify under oath and be subject to cross-examination. Indeed, even if the government elicits the inculpatory portion of the defendant's oral statement from a witness, the defendant is not entitled to elicit any exculpatory portion on cross-examination. *Ortega*, 203 F.3d at 682. The rule of completeness, Fed. R. Evid. 106, has no place in this analysis since it applies only to written or recorded statements. *Id.*

**E. Statements Offered for a Non-Hearsay Purpose**

A statement is hearsay if it is (1) an assertion that (2) is made out of court and (3) is offered to prove the truth of the matter asserted. *See* Fed. R. Evid. 801(c). Many out of court statements are not hearsay because they either are not assertions, or they are not offered to prove the truth of the matter asserted. *United States v. Oguns*, 921 F.2d 442, 449 (2d Cir. 1990) (questions are not assertions and are thus not hearsay). Furthermore, many statements that meet the definition of hearsay are admissible under one or more of the many exceptions to the hearsay rule.

In this case, the United States may offer out of court statements, not to prove the truth of the matters asserted, but merely to give context to the defendant's statements. Therefore, the statements would not constitute "hearsay" within the definition of Rule 801. *United States v. Catano*, 65 F.3d 219, 225 (1st Cir. 1995) (informant's part of conversation with agent was not hearsay, because it was offered for context and not to prove the truth of the informant's statements). Specifically, statements made by persons with whom Thompson communicated on social media or in texts are not hearsay if they



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

are not offered for their truth, but rather to provide context for statements made by Thompson.

**F. Admissibility of Summary Charts**

The investigation and prosecution of this case has involved extensive review of voluminous computer records, including computer logs. The government may present some of this evidence in the form of summary testimony and charts. The government has provided the defense with all the underlying materials in its possession (including images of Thompson's digital devices).

Federal Rule of Evidence 1006 provides that: "[t]he proponent may use a summary, chart, or calculation to prove the content of voluminous writings, recordings, or photographs that cannot conveniently be examined in court." The proponent of a summary must establish that the underlying materials cannot be conveniently examined in court, and that they are admissible at trial, as conditions precedent to introduction of the summary into evidence. *Amarelu v. Connell*, 102 F.3d 1494, 1516 (9th Cir. 1997). The proponent of a summary also must establish that the underlying documents were made available to the opposing party for inspection. *Paddack v. Dave Christensen, Inc.*, 745 F.2d 1254, 1259 (9th Cir. 1984). Summaries must fairly represent the underlying documents, and their admission into evidence is left to the trial court's discretion. *Davis & Cox v. Summa Corp.*, 751 F.2d 1507, 1516 (9th Cir. 1985), *superseded on other grounds by Northrup Corp. v. Triad Intern. Mktg., SA*, 842 F.2d 1154 (9th Cir. 1988).

Rule 1006 does not require that it literally be impossible for the fact finder to examine the underlying records before a summary may be admitted. *United States v. Stephens*, 779 F.2d 232, 238-39 (5th Cir. 1985). Rather, Rule 1006 contemplates that summaries of voluminous records may be used without introducing each and every underlying document into evidence. *United States v. Scales*, 594 F.2d 558, 562 (6th Cir. 1979). Furthermore, the fact that some of the underlying documents are already in evidence does not mean that they can be "conveniently examined in court." *United Stephens*, 779 F.2d at 239.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

The Ninth Circuit has affirmed the admission as substantive evidence of a wide variety of summary charts pursuant to Rule 1006 where such charts are based on the sponsoring witnesses' out-of-court review of voluminous evidence. *See, e.g.*, *United States v. Shirley*, 884 F.2d 1130, 1133 (9th Cir. 1989) (DEA agent presented chart summarizing information about telephone calls made to and from phones associated with defendants, relying on review of phone records, rental records, jail records, and other information); *United States v. Meyers*, 847 F.2d 1408, 1412 (9th Cir. 1988) (chart summarizing phone records and law enforcement surveillance reports); *United States v. Catabran*, 836 F.2d 453, 456-58 (9th Cir. 1988) (charts summarizing voluminous computer printouts and inventory records in bankruptcy fraud prosecution); *United States v. Gardner*, 611 F.2d 770, 776 (9th Cir. 1980) (IRS agent presented chart summarizing assets, liabilities, and expenditures of defendant in tax prosecution).

All of the requirements for admission of summary charts are met in this case. If the government were to introduce all of the relevant computer records, the jury would be faced with reviewing masses of forensic information, most of it incomprehensible to a layman. Any summaries that the government offers will fairly present the underlying evidence. As a result, any summary exhibits should be admitted.

**G. Defense Exhibit List**

The Government understands that the defense intends to introduce much of its case through the cross-examination of government witnesses. As Judge Jones recently held, and numerous other courts in this Circuit previously have held, a criminal defendant's case-in-chief includes evidence that the defendant seeks to introduce by cross-examining government witnesses. *See United States v. Louie Sanft et al.,* Order, at 4, No. CR19-0258RAJ (W.D. Wash., Nov. 12, 2021) (Docket No. 107). As a result, exhibits that the defense intends to introduce on cross examination (other than purely for impeachment) must be included on defendant's exhibit lists and provided to the government when exhibits are due. *See id.* The government has notified the defense of Judge Jones' order. To the extent that the defense fails to include on its exhibit list, and



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

in its exhibit binders, exhibits that it intends to use on cross-examination (other than exhibits that are purely impeachment exhibits), the government will oppose the use or admission of those exhibits at trial.

**H. Jury Nullification/Selective Prosecution**

During a meeting regarding motions *in limine*, the government indicated that it intended to file a motion precluding the defense from making any argument seeking jury nullification or arguing that the defendant had in any way been selectively prosecuted. The defense agreed that it would not make any jury-nullification or selective-prosecution arguments. As a result, and in reliance on that representation, the government is not filing a motion relating to such arguments.

The government notes that it would be improper for the defense to make any argument concerning the fact that defendant faces incarceration if convicted. "It has long been the law that it is inappropriate for a jury to consider or be informed of the consequences of their verdict." *United States v. Frank*, 956 F.2d 872, 879 (9th Cir. 1992). Information about penalties draws the attention of the jury away from its chief function as the trier-of-fact, opens the door to compromise verdicts, and confuses the issues to be decided. *United States v. Olano*, 62 F.3d 1180, 1202 (9th Cir. 1995).

Accordingly, it would be improper for the defense to make any reference to Thompson's potential punishment in the presence of the jury at any point in the proceedings. References to penalties could be as overt as "You understand the defendant is facing decades in prison if convicted," or more subtle, such as "the defendant is facing a lot of time," "this case has serious consequences for the defendant," "the defendant's liberty is at stake in this trial," or "your decision will have consequences for a long time to come." The Court should not permit any such statements by the defense.

**I. Video Testimony of Clint Popetz**

One of the government's witnesses, Clint Popetz of 42 Lines, Inc., currently lives in Canada, where he is in the process of applying for a work permit. Mr. Popetz cannot leave Canada while his application is pending. As a result, the government offered the



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

defense the option of having Mr. Popetz testify by videoconference, or of the government bringing a different witness from 42 Lines, Inc., to testify in person. The defense indicated that it preferred to have Mr. Popetz testify remotely. As a result, the government asks that Mr. Popetz be permitted to testify by videoconference, with the agreement of the parties.

**J. Exclusion of Witnesses**

Pursuant to Rule 615 of the Federal Rules of Evidence, the government respectfully requests that witnesses be excluded from the courtroom, with the exception of FBI Special Agent Joel Martini, who is a case agent and who should be permitted to sit at counsel table. *United States v. Thomas*, 835 F.2d 219, 222-23 (9th Cir. 1987); *see also United States v. Machor*, 879 F.2d 945, 953-54 (1st Cir. 1989).

## V. FORFEITURE

The United States seeks forfeiture in this case and provided notice to Defendant Thompson of this intent in the Indictment, Superseding Indictment, and the Second Superseding Indictment (Docket Nos. 33, 102 & 166), as required by Fed. R. Crim. P. 32.2(a). Specifically, the United States seeks to forfeit from Defendant:

1) A sum of money in the amount of approximately $10,014.00, reflecting the proceeds Defendant obtained from the Wire Fraud Scheme (Count 1). All proceeds of the Wire Fraud Scheme are forfeitable pursuant to 18 U.S.C. § 981(a)(1)(C), by way of 28 U.S.C. § 2461(c).
2) A sum of money in the amount of approximately $10,014.00, reflecting the proceeds Defendant obtained from Computer Fraud and Abuse (Count 8). All proceeds of this offense are forfeitable pursuant to 18 U.S.C. § 982(a)(2)(B) and 1030(i).
3) Any property used or intended to be used to commit or to facilitate the commission of Computer Fraud and Abuse (Counts 2, 4-8), and any property used or intendeds to be used to commit the commission of Access Device Fraud (Count 9). This property, which includes the electronic devices



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

identified below, is forfeitable pursuant to 18 U.S.C. § 982(a)(2)(B) and 1030(i) (Counts 2, 4-8) and pursuant to 18 U.S.C. § 982(a)(2)(B) and 1029(c)(1)(C) (Count 9):

a. Dell Laptop S/N: JKQKJM2 with power cord; and

b. White Desktop Computer Custom Built.

The United States expects the evidence at trial will establish that Defendant Thompson obtained approximately $10,014.00 in proceeds from the Wire Fraud Scheme and the Computer Fraud and Abuse offenses. The Wire Fraud scheme covers the same time period as the other offenses and encompasses the same proceeds. As a result, the United States only seeks forfeiture of that single amount, even if the Defendant is convicted both of Wire Fraud (Count 1) and Computer Fraud and Abuse (Count 8). The United States also expects the evidence at trial will establish that Defendant used, or intended to use, the electronic devices identified above to commit the Computer Fraud and Abuse and Access Device Fraud offenses.

**Legal Standard for Forfeiture.**

Criminal forfeiture is a form of punishment that is imposed as part of a criminal sentence. *Libretti v. United States*, 516 U.S. 29, 39 – 40 (1995). For the government to criminally forfeit property, there must be a predicate criminal conviction, a statute authorizing forfeiture for the crime of conviction, and evidence to support the statutorily required nexus between the property and the crime of conviction. *See e.g., United States v. Garcia-Guizar,* 160 F.3d 511, 518 – 20 (9th Cir. 1998) (reviewing these requirements). With respect to the required nexus, the government must establish the forfeitability of the relevant property by a preponderance of the evidence. *United States v. Martin,* 662 F.3d 301, 307 (4th Cir.2011); *see also United States v. Rutgard*, 116 F.3d 1270, 1293 (9th Cir. 1997); *United States v. Hernandez-Escarsega,* 886 F.2d 1560, 1576 – 77 (9th Cir. 1989).

In other words, depending on the relevant forfeiture statute, the government must present evidence that establishes the relevant property is, "more likely than not," forfeitable as *proceeds* of the crime and/or property *used, or intended to be used, to*



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

*commit or to facilitate* the crime. This lower standard of proof "is constitutional because the criminal forfeiture provision does not itself describe a separate offense but is merely an 'additional penalty' for an offense that must be proved beyond a reasonable doubt." *United States v. Garcia-Guizar,* 160 F.3d at 518 (citing *United States v. Hernandez-Escarsega,* 886 F.2d at 1577).

Here, there is statutory authority to forfeit the *proceeds* the Defendant obtained from the Wire Fraud Scheme (Count 1), pursuant to 18 U.S.C. § 981(a)(1)(C) (by way of 28 U.S.C. § 2461(c)), and from the Computer Fraud and Abuse offense (Count 8), pursuant to 18 U.S.C. § 982(a)(2)(B) and 1030(i). As permitted by Fed. R. Crim. P. ("Rule") 32.2 and approved in case law, the United States seeks to forfeit these proceeds in the form of "personal money judgments" entered against the Defendant. *See* Rule 32.2(b)(1)(A) and *United States v. Nejad*, 933 F.3d 1162 (9th Cir. 2019) (affirming a district court's authority to enter forfeiture money judgments and reciting circuit precedent). The government typically forfeits a money judgment when the Defendant has spent or otherwise disposed of the criminal proceeds, so they are no longer available to forfeit directly. *See United States v. Nejad,* 933 F.3d at 1165 (recognizing the necessity of forfeiture money judgments in this circumstance and holding "a contrary rule … would allow an insolvent defendant to escape the mandatory forfeiture penalty Congress has imposed simply by spending or otherwise disposing of his criminal proceeds before sentencing").

There is also statutory authority to forfeit any property *used, or intended to be used, to commit or to facilitate* the Computer Fraud and Abuse offenses (Counts 2, 4-8), pursuant to 18 U.S.C. § 982(a)(2)(B) and 1030(i), and any property *used or intended to be used to commit* the Access Device Fraud (Count 9), pursuant to 18 U.S.C. § 982(a)(2)(B) and 1029(c)(1)(C).

Forfeiture for all of these offenses is a mandatory part of any criminal sentence. *See* 28 U.S.C. § 2461(c) and 18 U.S.C. § 982(a)(1) (both providing the court *shall order* forfeiture when sentencing a defendant on these charges). The United States expects the



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

evidence at trial will establish, to a preponderance, the *proceeds* the Defendant obtained from these offenses, the property the Defendant *used or intended to be used to commit or to facilitate* the Computer Fraud and Abuse offenses, the property the Defendant used or intended to be used to commit the Access Device Fraud offense, and the nexus between the identified property and the Defendant's offenses.

**Forfeiture Process.**

Rule 32.2 sets out the procedures for determining the forfeitability of property in a criminal case. Forfeitures are decided after a guilty verdict is returned on a count that supports the forfeiture. *See* Rule 32.2(b)(1)(A). At that juncture, the specific question for the fact finder is "whether the government [has established the] requisite nexus between the property and the offense." Rule 32.2(b)(1)(A). Although a defendant has a right for a jury to determine the forfeitability of specific property, such as the electronic devices ((Rule 32.2(b)(5)), no such right exists for a forfeiture money judgment. The forfeiture of a sum of money is determined by the court, not the jury. *See* Rule 32.2(b)(1)(A) ("If the government seeks a personal money judgment, the court must determine the amount of money that the defendant will be ordered to pay."); *see also United States v. Tedder,* 403 F.3d 836, 841 (7th Cir. 2005) ("Rule 32.2 does not entitle the accused to a jury's decision on the amount of the forfeiture") and *United States v. Phillips,* 704 F.3d 754, 771 (9th Cir. 2012) ("Given that the only issue here was a monetary forfeiture, no jury determination was necessary.").

As forfeiture is determined post-conviction, and is considered part of sentencing, the rules of evidence do not strictly apply to forfeiture proceedings. *See e.g., United States v. Hatfield,* 795 F. Supp.2d 219, 229 – 30 (E.D.N.Y. 2011) (holding neither the Federal Rules of Evidence nor *Daubert* apply to forfeiture hearings) and *United States v. Creighton,* 52 Fed. Appx. 31, 35-36 (9th Cir. 2002) ("hearsay evidence is permissible at sentencing and does not, *per se*, lack sufficient indicia of reliability"). The fact finder may consider any evidence that is "relevant and reliable." Fed. R. Crim. P. 32.2(b)(1)(B). This includes any evidence presented by the parties during trial on the



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

substantive criminal offenses. *See id.* ("The court's [or jury's forfeiture] determination may be based on evidence already in the record …."); *see also United States v. Newman*, 659 F.3d 1235, 1244 – 45 (9th Cir. 2011) (same).

If the Defendant is convicted of one or more of the identified offenses, the United States expects to present the forfeiture case in a supplemental proceeding pursuant to Fed. R. Crim. P. 32.2(b)(1). The United States is willing to waive its right to retain the jury for that proceeding and have the Court decide the forfeitures. *See* Fed. R. Crim. P. 32.2(b)(5). If, however, the Defendant is unwilling to waive, the United States is prepared to present the forfeiture case (for the electronic devices) to the jury. For use in that proceeding, the United States is submitting proposed forfeiture jury instructions and a special forfeiture verdict form. The Court, not the jury, determines the sum of money to be forfeited. For this reason, the jury instructions and special verdict form do not address the forfeiture of a sum of money.

In the forfeiture proceeding, the United States expects to rely primarily on the testimony and evidence introduced during the guilt/innocence phase of trial. The United States expects testimony and related exhibits presented in its case-in-chief will establish that Defendant obtained approximately $10,014.00 in proceeds from the Wire Fraud Scheme (Count 1) and Computer Fraud and Abuse charged in Count 8, and that Defendant used, or intended to use, the identified electronic devices to commit or to facilitate the fraud offenses charged in Counts 2, 4-9. The United States expects to present argument with respect to the forfeiture of the identified property, but it does not expect to present substantial additional testimony or exhibits. The United States reserves its right, however, to offer alternative arguments and evidence in support of forfeiture, and to take different positions with respect to forfeiture, as necessary to respond to developments at trial.

//

//

//



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

## VI. CONCLUSION

The government is not aware of other legal issues that are likely to arise during the course of this trial. If other issues do arise, the government requests the opportunity to address those issues by way of a supplemental brief or briefs.

DATED: March 24, 2022.

NICHOLAS W. BROWN
United States Attorney

*s/ Andrew C. Friedman*
*s/ Jessica M. Manca*
*s/ Tania M. Culbertson*
ANDREW C. FRIEDMAN
JESSICA M. MANCA
TANIA M. CULBERTSON
Assistant United States Attorneys
700 Stewart Street, Suite 5220
Seattle, Washington 98101
Phone: (206) 553-7970
E-mail: Andrew.Friedman@usdoj.gov
Jessica.Manca@usdoj.gov
Tania.Culbertson@usdoj.gov